LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Information Security for Executives

A Guide for Leaders

Fiscal Year 2013

Information Security for Executives

- Introduction
- Information Security Overview
- Information Security Policy and Governance
- Data Protection
- Security and Your Business
- Summary
- Appendix

Introduction

Executive Introduction

Welcome to Information Security for Executives

"*As an executive of the Department of Health and Human Services (HHS), securing the Department's information and protecting the privacy of the citizens we serve should be one of your top priorities.*"

Frank Baitman
Chief Information Officer (CIO), HHS

Introduction

What happens if….

- A story appears in the national news about HHS data being stolen or disclosed to unauthorized personnel?
- The public loses confidence in HHS because of a security breach involving personal data?
- Criminals hack into HHS networks and steal information, threatening the privacy and financial security for millions of people?

Introduction

Could a Data Breach Happen at HHS?

YES!

Unfortunately, data breaches are a consistent threat to the Department. Any time information systems are compromised it has a negative impact on HHS' mission and reputation.

As an HHS executive, you must lead by example and establish a culture of protection for sensitive data within your organization.

Protection of HHS proprietary information systems and client and employee personally identifiable information must be a priority in your daily actions.

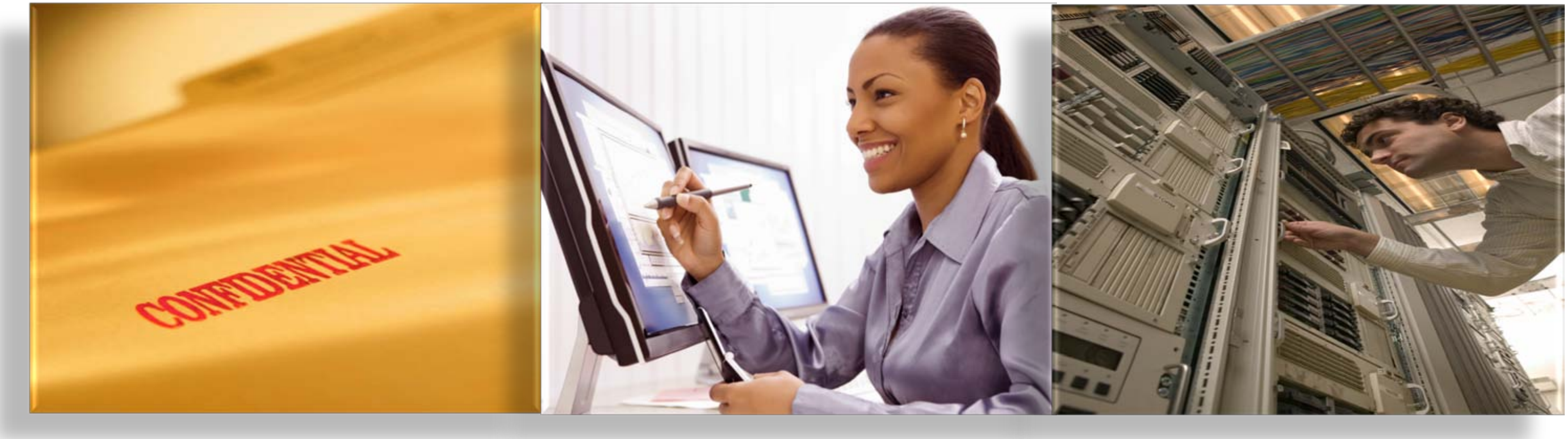
Introduction

Objectives

At the end of this course you will be able to:

- Define information security and emerging threats.
- Identify governing bodies and legislative drivers for protecting information security.
- Define privacy and why it is important to protect information technology (IT) assets.
- Recognize common threats to IT assets and know how to protect them.
- Understand your role and responsibilities as an HHS executive in the areas of information security and privacy.
- Identify where to locate HHS information security and privacy resources.

Information Security Overview



Information Security Overview

What is Information Security?

Information security (IS) – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- Information security is achieved through implementing technical, management, and operational measures designed to protect the **confidentiality, availability, and integrity** of information.
- The goal of an IS program is to **understand, manage, and reduce the risk to information** under the control of the organization.

> "Leaders need to be security conscious and to treat adequate security as a non-negotiable requirement of being in business." CERT Program, Carnegie Mellon University

Information Security Overview

Key Concepts

There are three elements to protecting information:

- **Confidentiality** – Protecting information from unauthorized disclosure to people or processes.
- **Availability** – Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users.
- **Integrity** – Assuring the reliability and accuracy of information and IT resources.

Your bank ATM is a good example of an information system that is confidential, available, and has integrity.

- The ATM is available for you to access your money 24 hours a day.
- Your information and account balance is kept confidential and only displayed after entering your PIN.
- The account balance is accurate and reliable; otherwise you would overdraw the account.

Information Security Overview

Key Concepts

Threats and vulnerabilities put information assets at risk.

- **Threats** – the potential to cause unauthorized disclosure, changes, or destruction to an asset.
  - Impact: potential breach in confidentiality, unavailability of information, and integrity failure
  - Types: natural, environmental, and man-made

- **Vulnerabilities** – any flaw or weakness that can be exploited and could result in a breach or a violation of a system’s security policy.

Information Security Overview

Key Concepts

Controls help protect IT assets.

- **Controls** – countermeasures to avoid, mitigate, or minimize security risks.
- There are three types of controls:
  - **Management controls** involve policy or procedure to manage risk and information system security.
  - **Operational controls** rely on people to perform certain actions to ensure security.
  - **Technical controls** are primarily implemented and executed through mechanisms contained in the hardware, software, or firmware of the information system.
- **Risk management** is the process of identifying threats and vulnerabilities to IT assets and establishing acceptable controls to reduce the likelihood of a security breach or violation.

Information Security Overview

Key Concepts

Privacy – A set of fair information practices to ensure that an individual's personal information is accurate, secure, and current, and that individuals are informed how their personal data will be used.

- **Personally Identifiable Information (PII)** – Any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains.
- **Protected Health Information (PHI)** – Information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Information Security Policy and Governance

Information Security Policy and Governance

Federal Governance

The following legislation and guidance provides the backbone to governance that protects federal information and systems.

Federal Information Security Management Act (FISMA) of 2002	OMB Circular A-130, Management of Federal Information Resources	National Institute of Standards and Technology (NIST) Special Publications (SP)
▸ Designates Office of Management and Budget (OMB) with the oversight of federal agencies' IT security implementation. ▸ Provides a comprehensive framework for securing federal government information resources.	▸ Establishes a minimum set of security controls to be included in federal IT security programs. ▸ Assigns federal agency responsibilities for the security of automated information.	▸ Issues standards and guidelines to assist federal agencies in implementing these regulations. ▸ Provides these agencies with an infrastructure for overseeing implementation of required practices.

Information Security Policy and Governance

Department Governance

- **HHS Headquarters (HQ)** sets programmatic direction by providing an enterprise-wide perspective, facilitating coordination among key stakeholders, setting standards and providing guidance, and supporting streamlined reporting and metrics capabilities.

- **Operating Divisions (OpDivs)** implement programs that meet specific business needs, provide business/domain expertise, participate in establishing an enterprise-wide baseline, manage implementation at the OpDiv level, and manage ongoing operations.

- **HHS Cybersecurity Program** is the Department’s information security program. Oversight is provided by the Office of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO).

Information Security Policy and Governance

Department Governance

- The *HHS-OCIO Policy for Information Systems Security and Privacy* provides direction on developing, managing, and operating an IT security program to the OPDIVs and Staff Divisions (StaffDivs).

- The *HHS-OCIO Policy for IT Security and Privacy Incident Reporting and Response* establishes the HHS Computer Security Incident Response Center (CSIRC) as the primary entity in the Department responsible for maintaining Department-wide operational IT security situational awareness and for determining the overall operational IT security risk posture of HHS.

Information Security Policy and Governance

Department Governance

- OpDivs and StaffDivs may have additional policies and programs specific to their operating environment, however they shall comply with and support the implementation of a Department-wide IT security and privacy program.

Information Security Policy and Governance

The HHS Executive’s Security Role

- ✓ Set explicit expectations for protecting security and empower employees to make protecting the information, health, safety, and well-being of the American people their personal mission.
- ✓ Allocate resources to ensure that systems are adequately protected to prevent compromise of sensitive information.
- ✓ Ensure that information security and privacy are integrated into all information systems development activities.
- ✓ Incorporate security into your day-to-day business – make it a routine topic in staff meetings and when making management decisions.
- ✓ Ensure that employees receive the training they need and are held accountable for protecting sensitive information.
- ✓ Heighten awareness on how to quickly identify security incidents and the proper response to an incident.

Data Protection

Data Protection

Data Breaches in the News

CFTC Data Breach Risks Employees' Social Security Numbers
Bloomberg Businessweek, June 25, 2012

The U.S. Commodity Futures Trading Commission suffered a data breach in May, putting at risk Social Security numbers and personal information of employees of the country's top derivatives regulator.

Laptop lost with data for more than 2,000 patients, Boston Children's reports
The Boston Globe, May 22, 2012

While at a conference in Buenos Aires, a Boston Children's Hospital employee lost a laptop containing a file with information about 2,159 patients, including names, birth dates, diagnoses, and treatment information. The laptop was password protected but not encrypted, according to a hospital press release.

Data breaches up 19 percent, GAO reports
Federal Times, July 31, 2012

Federal data breaches jumped 19 percent last year, the Government Accountability Office said Tuesday.
There were roughly 13,000 incidents reported by agencies in 2010 involving unauthorized disclosures of personally identifiable information — last year, that figure shot up to 15,500, Greg Wilshusen, GAO's director of information security issues, told the Senate subcommittee on government management oversight Tuesday at a hearing.

Data Protection

Common Cybersecurity Threats

- Malware
- Viruses
- Insider Threats
- Spyware
- Hackers
- Theft or loss of sensitive data
- Internet and Email Scams
- Phishing

Data Protection

What is a Cyber Attack?

Cyber Attacks – A malicious attempt to undermine or compromise the function of a computer-based system, or attempt to track the online movements of individuals without their permission.

Attacks Can be Costly

The Ponemon Institute benchmarked 50 organizations - the median annualized cost of a cyber attack is $5.9 million/year.

The Department of Defense (DoD) detects three million unauthorized “scans”- or attempts by possible intruders to access official networks every day.

Attacks are Pervasive and Common

Attacks Don’t Have to be Costly

According to the Ponemon Institute, a strong security posture moderates the cost of cyber attacks

Data Protection

Cyber Attacks – Not Science Fiction Anymore

April 2012 - Utah Medicaid clients had their information exposed by a hack of an improperly protected Utah Department of Health computer server. The breach was discovered when an unusual amount of data was found to be streaming out of the server.

The Utah Department of Health reported that nearly 280,000 people had their Social Security numbers exposed by the breach. An additional 500,000 victims did not have their Social Security numbers exposed, but had some form of personal information exposed, such as date of birth, name, and address. Two out of three of those who were affected were children. The cost of working with the credit-reporting company, Experian, to contain the breach is estimated to be $460,000.

Information Source:
PHIPrivacy.net

Data Protection

Preventing Cyber Attacks

Information assets have become a great source of value and wealth for individuals with malicious intent. Cyber attacks are a dangerous threat to HHS networks and data, however there are some steps you and your staff can take to prevent them.

<u>How to combat cyber attacks:</u>

- Follow Department and OPDIV information security and privacy policies and controls at all times.
- Ensure that anti-virus software and patches are up to date on all computers and laptops.
- Ensure that laptops and mobile devices are encrypted with federally approved software.
- Never share passwords with anyone.
- Report slow running applications. It could be a sign of a computer virus.

Data Protection

Mobile Device Loss and Theft

Cyber attacks are a dangerous threat to HHS networks and data, however a large number of breaches occur because of loss or theft of mobile devices.

How to combat mobile device loss and theft:

- Never leave laptops, cell phones, or other mobile devices unattended – especially when travelling.
- When away from your desk, use a computer lock for your laptop or place it in a locked cabinet.
- Mobile devices that contain PII must be encrypted.
- Completely shut down your laptop while in transit to enable encryption.
- Report lost or stolen devices *immediately*.

Data Protection

Social Engineering

- **Social engineering** is classically defined as the art of manipulating and exploiting human behavior to gain unauthorized access to systems and information for fraudulent or criminal purposes.
- Social engineering attacks are more common and more successful than computer hacking attacks against the network.

Data Protection

Social Engineering

- Social engineering is a growing threat to data security and privacy.
- Criminals use natural human instincts like trust or the desire to help to manipulate people to divulge valuable information (like passwords).
- Criminals can bypass network firewalls and building access systems to steal data and disrupt operations with a successful social engineering attack.

How to combat social engineering:

- Be careful about discussing work, your family, or personal information in public. You never know who is listening.
- Be cautious of the personal information that you share on social media sites like Facebook. Criminals can use the information you post in a social engineering scam.

Data Protection

Phishing

- **Phishing** is an attempt to obtain personal information such as passwords, usernames, and credit card numbers by masquerading as a trustworthy entity in an electronic communication.
- **Whaling** is a phishing attack directed at senior executives in an attempt to gain access to high-value information like sensitive customer data or proprietary business information. A successful attack can be devastating because it involves high-level access to an organization’s network systems.

How to combat Phishing Scams:

- Do not respond to email or text messages that ask for personal information like credit card numbers, Social Security numbers, passwords, etc.
- Do not click on links provided in email or text messages. The link could be for a fake or spoof site, which looks legitimate, but is set up by criminals to steal your information.
- Review your financial statements at least once a month for unauthorized charges.

Data Protection

Potential Impacts Resulting from the Loss of Sensitive Information

Failure to exercise due diligence in protecting sensitive information can result in:

- ✘ Reputation damage for HHS
- ✘ Loss of trust in HHS
- ✘ Legal ramifications for HHS
- ✘ Injury or damage for those who have had their private information exposed
- ✘ Potential financial ramifications for those affected
- ✘ Employee discipline
- ✘ Criminal and/or civil penalties for employees involved

Data Protection

Protect HHS Data and Equipment

In order to protect HHS and personal property:

- Lock computer workstations when not in use;
- Lock up documents and files that contain PII;
- Keep watch over laptops and other portable devices while travelling;
- Use authorized mobile devices with encryption to store PII;
- Always encrypt emails that contain PII; and
- Never throw papers or equipment containing PII or sensitive information in the trash.
  - Shred the papers and contact the IT department to collect and destroy the equipment.

Security and Your Business

Security and Your Business

How Does Security Impact My Business?

- Enterprise Performance Lifecycle (EPLC)
- Capital Planning and Investment Control (CPIC)
- Risk Management Framework
- Training & Awareness
- Contract Oversight
- Inappropriate Behavior

Security and Your Business

Enterprise Performance Lifecycle (EPLC)

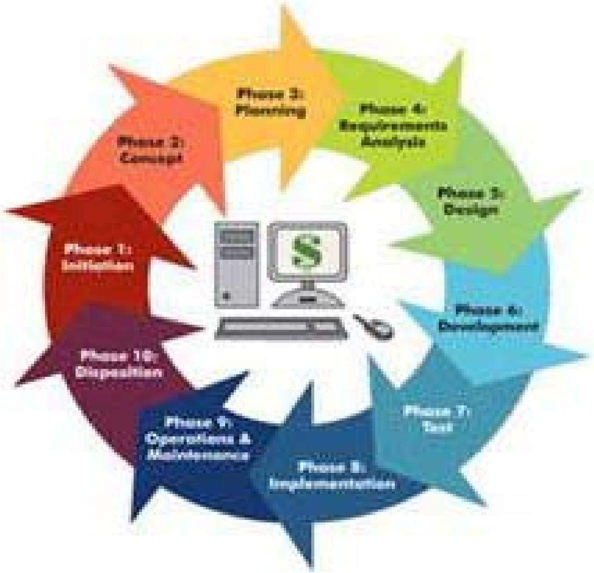
- **What is EPLC?**
  - HHS' IT project management methodology that incorporates best government and commercial practices through a consistent and repeatable process.
  - Standard structure for planning, managing and overseeing IT projects over their entire life cycle.
  - Process that maximizes project and investment alignment with Departmental and OPDIV strategic goals.

- **What is the Security requirement?**
  - Security must be incorporated in all phases of EPLC in order to reduce system risk and enhance the confidentiality, integrity and availability of HHS IT systems.

Security and Your Business

Enterprise Performance Lifecycle

- For more information on the EPLC framework see “Appendix E: Security Deliverables” of the *Enterprise Performance Life Cycle*



EXECUTIVE ACTION:

Ensure that security is incorporated into all phases of the EPLC.

Security and Your Business

Capital Planning and Investment Control (CPIC) Process

- **What is CPIC?**
  - CPIC is the primary process for making investment decisions, assessing investment process, effectiveness, and refining related policies and procedures.
  - CPIC ensures fiscal accountability of Exhibit 300 business cases.
  - CPIC integrates information security into the CPIC process to avoid budgeting ramifications.
  - CPIC utilizes the EPLC framework to strengthen measureable results for IT investments.

EXECUTIVE ACTION:

Ensure that information security is integrated into the CPIC process.

Security and Your Business

Risk Management Framework

- OMB requires that agencies assess, select, and implement security controls that reduce the security risk associated with operating a federal information system. Agencies are also required to formally authorize federal information system operation and accept and/or mitigate any residual risks associated with their operation.

- Security authorization is an official decision of an agency designated official to accept the risk of operating the information system. This decision is based on the amount of residual risk to the organization after the implementation of security controls. Each agency or organization may have different levels of acceptable risk based on the sensitivity of the information in the system and their mission.

- The Risk Management Framework (RMF) outlined in NIST SP 800-37 Rev. 1 provides guidance to senior leaders on how to assess risk, implement controls, and authorize federal information systems.

EXECUTIVE ACTION:

Ensure that information security is integrated into systems and operating risk is acceptable per the overall risk strategy of the organization.

Security and Your Business

Training & Awareness

All system users must complete mandatory security awareness training and privacy awareness training before receiving system access.

- Security awareness training and privacy awareness training must be taken annually by employees, contractor personnel, interns and other non-government employees conducting business for or on behalf of the Department through contractual relationships or memoranda of agreement when managing, maintaining, and/or using government data or information systems.
- Role based training (RBT) is also required for individuals with significant security responsibilities (SSR).

EXECUTIVE ACTION:

Ensure the appropriate training of system users and staff with significant security responsibilities.

Security and Your Business

Contract Oversight

Executives must ensure that contracts and contractors support the security environment.

- The *Security and Privacy Guide for Information Technology Acquisition* provides information on the security requirements that must be included in contracts.
- Contractors must fulfill security training requirements.
- Non-disclosure agreements (NDA) must be signed by all system users with access to sensitive information.

EXECUTIVE ACTION:

Ensure that information security requirements are included in contract language throughout the procurement lifecycle.

Security and Your Business

Inappropriate Behavior

- Employees are permitted limited personal use of HHS IT resources. This personal use shall not result in loss of employee productivity, interference with official duties, or incur more than “minimal additional expense” to HHS.
- Viewing inappropriate websites, gambling online, and installing unauthorized software is considered inappropriate behavior.
- Refer to the HHS-OCIO Policy for Personal Use of Information Technology Resources for guidance on sanctions for misuse.
- Refer to the HHS Rules of Behavior (For Use of HHS Information Technology Resources) and your local OPDIV procedures.

EXECUTIVE ACTION:

Ensure employees are familiar with HHS’ policy for personal use of information technology resources.

Security and Your Business

Do You Have an Information Security Problem?

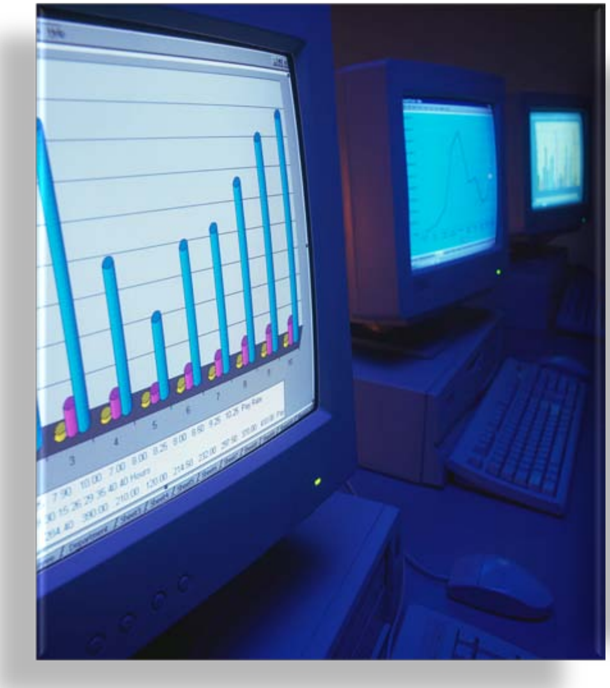
Watch out for these warning signs:

- You do not see regular reporting of security related metrics such as:
  - Accounts created/terminated according to corresponding hires and departures;
  - Plan of Action & Milestones* (POA&M) status updates;
  - Security awareness training percent complete; or
  - System authorization effort statuses.
- You do not see evidence of security being integrated across functional areas (HR, IT, etc.).
- You never hear of security incidents within your organization.

* A POA&M is a management tool for identifying, managing, and mitigating risks in an information system.

Incident Response

How to Handle a Security or Privacy Incident



Incident Response

What is an Incident?

An incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Source: FIPS Publication 200 Minimum Security Requirements for Federal Information and Information Systems

Incident Response

Federal Legislation and Guidance

The following Federal legislation and guidance govern incident response and reporting:*

- The Privacy Act of 1974
- OMB M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- NIST SP 800-53 Rev 3 *Recommended Security Controls for Federal Information Systems and Organizations*
- NIST SP 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*

*An extensive list of legislation and guidance is located at: http://intranet.hhs.gov/it/cybersecurity/privacy/index.html.

Incident Response

HHS Incident Response Policies

Encourage awareness and compliance with applicable Department policies for protecting sensitive information and reporting a security incident:

- HHS Incident Notification Process
- HHS-OCIO Policy for IT Security and Privacy Incident Reporting and Responses
- Updated Departmental Standard for the Definition of Sensitive Information
- Standard for Encryption

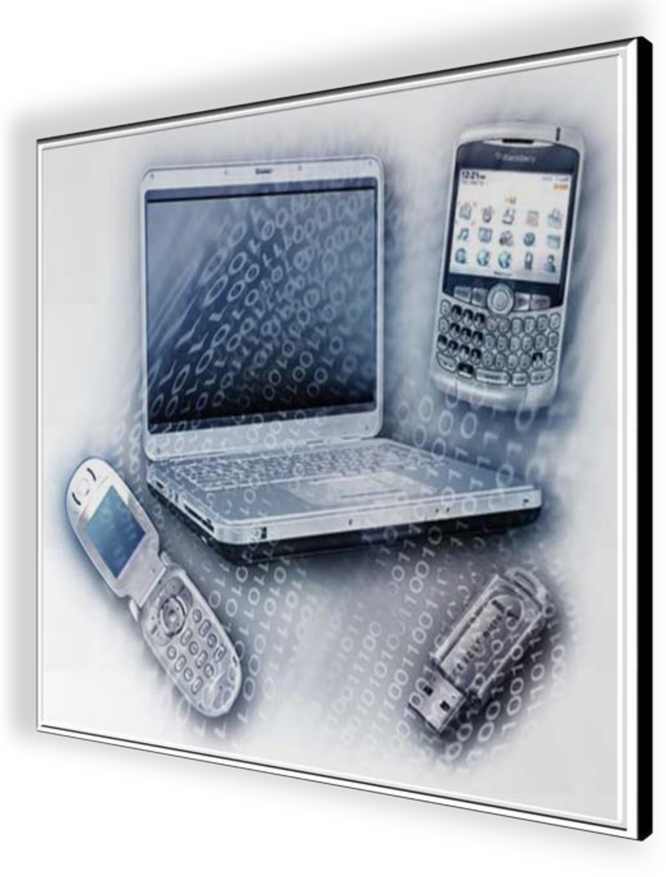
Contact your OPDIV CISO or Incident Response Team (IRT) to verify local incident notification procedures.

Incident Response

Protecting Sensitive Information

HHS personnel have a responsibility to:

- Protect sensitive HHS data.
- Protect the personal information of individuals.
- Protect individuals from harm that might be imposed upon them, if certain information were to be released without their consent.
- Encrypt mobile devices that store sensitive information with whole-disk encryption software.
- Encrypt emails that contain PII before sending.
- Immediately report suspected or confirmed loss, theft, or misuse of sensitive information or PII.



Incident Response

Responsibility for Reporting

Known and suspected incidents must be reported *immediately*. Do not delay reporting under any circumstance.

Reporting ensures HHS is meeting Federal requirements and can take immediate action to investigate. HHS must report known and suspected breaches to US-Computer Emergency Readiness Team (CERT) **within one hour of discovery.**

Incident Response

When to Report an Incident

- Report any situation that could compromise the confidentiality, availability or integrity of data in any format (electronic, paper, or oral communications).
- Common situations include:
  - Loss, damage, theft, or improper disposal of HHS equipment, documents, or files;
  - Disclosing PII to a person who is not authorized to have it (e.g., faxing, emailing, or sending PII to the wrong person);
  - Unauthorized access (e.g., an employee accessing PII that they should not have access);
  - Any security situation that could compromise PII (e.g., virus, phishing email, social engineering attack); and
  - Slow running computers or applications that are not performing correctly are a sign of a virus or malware and should be reported for further investigation.

Incident Response

How to Report a Data Breach

- Report to your OPDIV Computer Security Incident Response Team (CSIRT).
- You can also report directly to the HHS Computer Security Incident Response Center (HHS CSIRC).

	HHS CSIRC
Telephone	1-866-646-7514
Email Address	csirc@hhs.gov
Outlook Display Name	(CSIRC - HHS Computer Security Incident Response Center)

Summary

Summary

The HHS Executive’s Security Role

- ✓ Set explicit expectations for protecting security and empower employees to make protecting the information, health, safety, and well-being of the American people their personal mission.
- ✓ Allocate resources to ensure that systems are adequately protected to prevent compromise of sensitive information.
- ✓ Ensure that information security and privacy are integrated into all information systems development activities.
- ✓ Incorporate security into your day-to-day business – make it a routine topic in staff meetings and when making management decisions.
- ✓ Ensure that employees receive the training they need and are held accountable for protecting sensitive information.
- ✓ Heighten awareness on how to quickly identify security incidents and the proper response to an incident.

Summary

Objectives

You are now able to:

- Define information security and emerging threats.
- Identify governing bodies and legislative drivers for protecting information security.
- Define privacy and why it is important to protect your IT assets and investments.
- Recognize common threats to IT assets and know how to protect them.
- Understand your role and responsibilities as an HHS executive in the areas of information security and privacy.
- Identify where to locate HHS information security resources.

Congratulations

Congratulations!

You have completed the Information Security for Executives course.

Appendix

HHS Resources

- The **HHS Cybersecurity Program** is the Department‘s enterprise-wide information security and privacy program, helping to protect HHS against potential IT threats and vulnerabilities. The Program plays an important role in protecting HHS' ability to provide mission-critical operations, and is an enabler for e-government.
- HHS Cybersecurity Program Support provides assistance with IT security and privacy related issues. HHS Cybersecurity Program Support is staffed Monday through Friday from 8:00 AM to 5:00 PM eastern standard time (EST).

Web: HHS Cybersecurity Program

Phone: (202) 205-9581

E-mail: HHS.Cybersecurity@hhs.gov

Appendix

HHS Resources

- Information pertaining to the HHS Information Security and Privacy Program can be found at: http://www.hhs.gov/ocio/securityprivacy/index.html.
- Information pertaining to Federal cybersecurity and privacy legislation can be found at: http://www.hhs.gov/ocio/securityprivacy/pglandreports/polguidlegrep.html.
- The *HHS-OCIO Policy for Information Systems Security and Privacy* establishes comprehensive IT security and privacy requirements for the IT security programs and information systems of OPDIVs and STAFFDIVs within HHS.